(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 February 2002 (07.02.2002)

PCT

(10) International Publication Number
WO 02/11009 A1

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/KR01/01293

(22) International Filing Date: 30 July 2001 (30.07.2001)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
2000/43923 29 July 2000 (29.07.2000) KR

(71) Applicant *(for all designated States except US)*: **WOO-JOOWEB CO., LTD.** [KR/KR]; RM 1019 Hanshin Core Officetel, 11-9 Shincheon-dong, Songpa-gu, Seoul 138-733 (KR).

(71) Applicant *(for US only)*: **LIM, Jong, Min** [KR/KR]; Byuksan Apt. 106-404, Siheung 2-dong, Geumcheon-gu, Seoul 153-032 (KR).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **KIM, Bong, Se** [KR/KR]; 404-130 Mok-dong, Yangcheon-gu, Seoul 158-050 (KR).

(74) Agent: **CHU, Sung, Min**; Seoul Building, 114-31, Uni-dong, Chongro-gu, Seoul 110-350 (KR).

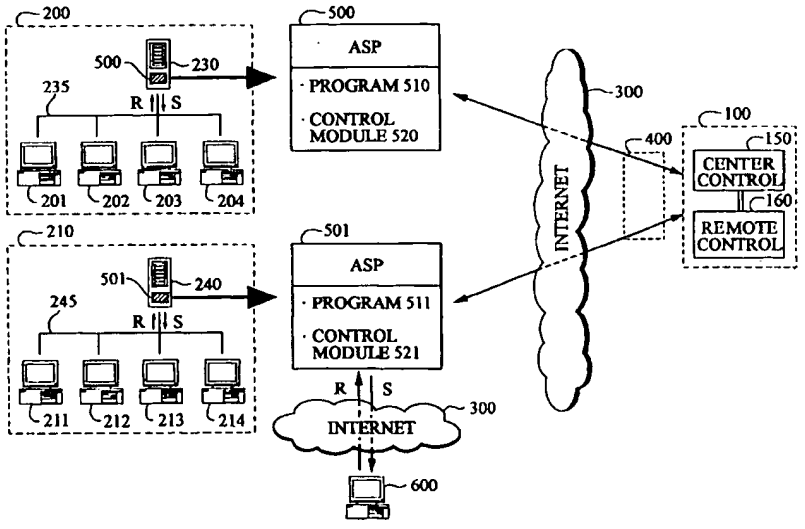
(81) Designated States *(national)*: CN, JP, US.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR PROVIDING APPLICATION SERVICES USING NETWORK TRAFFIC DISTRIBUTING SCHEME



(57) Abstract: An application service is provided using an efficient network of distributing traffic, thereby enhancing the data traffic in the ASP and drastically cutting down initial costs required for setting up an ASP data center and maintenance costs. A service request is received of application service data from a user via the Internet. It is then determined whether the user's information contained in the service request is valid based on the user information stored in a user database. A control signal containing a service permission or reject signal for the application service data is transmitted to the user module, according to the determined result The user module, responsive to the control signal, controls the access of the user to the application service data.

WO 02/11009 A1

SYSTEM AND METHOD FOR PROVIDING APPLICATION SERVICES USING NETWORK TRAFFIC DISTRIBUTING SCHEME

TECHNICAL FIELD

The present invention relates to providing off-site software applications and, in particular, to a system and method for providing the use of off-site applications through an efficient scheme of distributing network traffic.

BACKGROUND ART

In recent years, as the Internet becomes a most popular communications network, an application providing service using the global network has been drawing attention. An application service provider ("ASP") is a software rental service that allows customers to use remotely-stored applications via the Internet. In other words, ASP is a service (usually a business) that provides remote access to application programs across a network. A common example is a web site that other web sites access for accepting payment by credit card as part of their online ordering systems. Business application programs such as groupware, ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), SCM (Supply Chain Management), are remotely stored at the computer of an ASP service provider.

Fig. 1 is a schematic diagram of a conventional ASP service environment.

An ASP data center 100, representing an ASP service provider, includes customer servers 110-114, application servers 120-125, workstations 130-131, local area networks (LANs) 140-141, and a data center controller 150 for controlling these components.

The customer servers 110-114 are provided for customers. The customers connect to the customer servers

110-114 through the Internet 300. The customer servers provide home pages for customers, authenticate logins, and control the level of program access (open, read, write, and modify). A customer may use one or more of the customer servers 110-114.

The application servers 120-125 store various application programs and operate in conjunction with one or more of the customer servers that are related to access to or execution of application programs.

The workstations 130-131 control communications among a plurality of servers when the servers simultaneously are engaged to perform a task.

The LANs 140-141 are used to connect the servers and workstations of the ASP data center 100 in a network.

The ASP data center controller 150 controls and manages all the systems in the ASP data center 100. It may incorporate a firewall, a user authentication unit, an uninterruptible power system for protecting stored resources during a power failure, control units for controlling initialization, operation and termination of each of the servers.

The customers can use one or more of the servers and applications at the ASP data center 100 via the Internet 300. For example, each of numerical references 200 and 210, which is a user module registered as a customer of the ASP data center 100, includes local storage medium (LSMs) 230 and 240, respectively. The user module 200 includes a plurality of end users 201 to 204 as a member, and the user module 210 includes a plurality of end users 211 to 214 as a member.

In this conventional ASP, when an end user 201 wants to use a certain application installed in the application servers 120-125, it accesses the ASP data center controller 150 in the ASP data center 100 through the LSM 230 and the Internet 300. In response, the controller 150 performs an authentication procedure for

the user based on information on the end user 201(or the user module 200), which has been registered in a user database (not shown). If the user is authenticated, the controller 150 allows the end user 201 to access a customer server (110) that is related to program executions by application servers 120-123. In other words, the end user 201 can select one of programs installed in the application servers 120 to 123 via the customer server 110. Further, if necessary, it customizes interface and environment in order to establish a high speed and low cost computing environment. Another end user, for example the end user 211, can similarly use a desired program installed in the application server 125 through connection to the ASP data center 100 via the LSM 240 and the Internet 300. However, communication channels, marked with the reference numeral 400 in Fig. 1, are shared by all users due to the structure of the network. As a result, when a number of users simultaneously attempt to access the ASP data center 100 to use application services these channels must handle an extremely amount of traffic. In order to deal with this situation, it is necessary to provide an enough bandwidth, i.e., a high-speed Internet backbone, to the ASP data center 100 and to set up a stable system to prevent a system down.

In addition this conventional ASP data center 100 requires huge investment to acquire multiple servers, network equipment and the like. Costs for updating the center increase because it needs more human resources for maintenance and management as the number of customers and application services grow. IP address shortage is another growing pain. As a result, ASP providers must pay a high price for initial setting up and on-going maintenance of computer and network equipment.

DISCLOSURE OF THE INVENTION

It is, therefore, a primary objective of the present invention to provide a system and a method for implementing an application service provider (ASP) using an efficient network traffic distributed approach, thereby enhancing a traffic performance in the ASP and cutting drastically down primary costs required during the establishment of an ASP data center and maintenance costs thereof.

In accordance with one aspect of the present invention, there is provided a system for providing at least one of application services to a user, comprising: means disposed in a user module, for providing at least one of application services to the user; and means remotely located to the user module, for controlling the application services, and wherein application service data associated with the application services is stored in the providing means, and wherein the providing means is initially operated under the control of the controlling means, and is operated independent of the controlling means after the initial operation.

In accordance with another aspect of the present invention, there is provided a method in an application service system including a controller with a user database of storing information on a plurality of users therein and a user module having at least one of application service data, for remotely controlling the execution of the application service data using a communication network, comprising the steps of: (a) receiving a service request of the application service data from a user via the network; (b) determining whether the user's information contained in the service request is valid based on the user information stored in the user database; (c) transmitting a control signal containing a service permission or prohibition signal for the

application service data to the user module, according to the determined result at the above step (b); and (d) allowing, the user module, responsive to the control signal, to control the access of the user to the application service data.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other objects and features of the present invention will become apparent from the following description of preferred embodiments given in conjunction with the accompanying drawings, in which:

Fig. 1 shows a schematic diagram of a conventional ASP;

Fig. 2 is a schematic diagram of an ASP system in accordance with a preferred embodiment of the present invention;

Fig. 3 is a flowchart illustrating the operation of the application service remote controller shown in Fig. 2;

Fig. 4 is a flowchart illustrating the authentication key transmission process shown in Fig. 3;

Fig. 5 is a flowchart illustrating the banner transmission process shown in Fig. 3;

Fig. 6 is a flowchart which will be used to describe the operation of the ASP 500 shown in Fig. 2; and

Fig. 7 is a flowchart which will be used to describe the monitoring procedure between the ASP data center and the ASPs.

MODE OF CARRYING OUT THE INVENTION

The present invention will now be described in detail with reference to Figs. 2 to 6. In Figs. 2 to 6, like reference numerals will be used for like elements in Fig. 1.

Fig. 2 is a schematic diagram of an ASP system in

accordance with the present invention. Unlike the conventional ASP described above, the inventive ASP has a plurality of ASPs 500 and 501 disposed at local storage medium (LSMs) 230 and 240 within user modules 200 and 210 and an application service controller 160 is provided at the ASP data center 100 to remotely control the operation of the ASPs 500 and 501 via a communication network such as the Internet 300.

The ASPs 500 and 501 includes application programs 510 and 511 that the users want and application control modules 520 and 521 for controlling the application programs 510 and 511. An approach for providing the ASPs 500 and 501 in the LSMs 230 and 240 of the user modules 200 and 210 will be discussed. Typically, remotely obtaining a "write" function on an LSM through a communication channel requires an account given by the manager of the LSM. But this way is not practical. To solve this problem, the present invention is such that, if the remote application service controller 160 at the ASP data center 100 transmits a query to the application control module 520, the application control module 520 accesses the ASP data center 100 to download a specified file from the ASP data center 100. In other words, the application control module 520 installed in the LSM 230 is designed so that it detects a signal transmitted from the ASP data center 100 to connect to a server in the ASP data center 100. Specifically, the application control module 520 is preferably designed in a language that is transferable and independent of platforms so that it can operate under any operating system. The application control module 520 provides issues permission for a particular file and produces the characteristics of the file in HTML for display. It also creates a particular port through which the ASP data center 100 manages, modifies and deletes files on the side of users.

The number and types of application programs 510

and 511 may be selected according to requests from user modules 200 and 210.

The application control modules 520 and 521 each control all functions associated with the execution of the application programs 510 and 511. The "execution of the application program" refers to activation or reactivation of the application program 510 installed at the LSM 230. The application control module 520 receives an authorization or a rejection from the application service remote controller 160 for program execution. The application control module 520 may also receive an authentication key signal or an advertisement (e.g., banner) signal from the application service remote controller 160.

The application service remote controller 160 of the ASP data center 100 remotely controls the operation of the ASP 500 via the Internet 300. It establishes a user database (not shown) using indices such as a host name, IP address, which are received when the ASP 500 is installed in the LSM 230 on the user side. And it transmits the authorization or reject signal for the execution of an application program to the ASP 500 based on the user database, in the case it receives an application execution request from the LSM 230 of the user module 200 or needs to monitor the operation of the ASP 500. Alternatively, users may be classified into predefined types so that a different control signal can be transmitted to a different type. For example, users may be classified into paying customers and non-paying customers such that an authentication key is provided to the paying customers and a banner advertisement is transmitted to the non-paying customers.

Fig. 3 is a flowchart illustrating the operation of the application service remote controller 160 shown in Fig. 2. If a request for the execution of an application program 510, which is stored in the LSM 230 for example,

is received from the LSM 230 of the user module 200 (step S100), the remote controller 160 searches a user database (not shown) and extracts information on the user module 200 (step S110). Next, a decision is made to determine whether or not the user module 200 is previously registered as a customer (step S120). If the determined result is negative, the process is terminated. Otherwise, the remote controller 160 transmits an execution wait signal to the ASP 500 (step S140). Subsequently, a decision is made to check whether or not the user is a paying one (step S150). If so, the remote controller 160 transmits an authentication key to the ASP 500 (step S160). If the checked result is negative, the remote controller 160 transmits banner information to the ASP 500 (step S170). After the above step, the information obtained at steps S160 and S170 is in the database and the remote controller 160 determines whether, by a checksum, the authentication key and the banner information are deteriorated during the data transmission or by a file modulation in the LSM 230 itself (steps S180). The checksum process is performed by comparing the authentication key and the banner stored in the ASP data center 100 with that stored in the LSM 230. If these match, the remote controller 160 provides the execution permission signal for the application program 510 to the ASP 500 (step S190). Otherwise, it determines that an abnormal loading of program has taken place and terminates the process.

Fig. 4 is a flowchart illustrating the authentication key transmission process shown in Fig. 3.

If the user is determined as a paying one (step S150), the remote controller 160 searches a paying user database (DB) 166 (step S161) to determine whether the user is a new one (step S162). If positive, the remote controller 160 creates a user authentication key based on index information including a name of LSM and IP address,

and transmits it to the ASP 500 of the LSM 230 (step S163). In an ensuing step S164, the process stores the information of the LSM and the authentication key in the database 166 and goes to step S180 in Fig. 3. If the user was determined as a previously registered one (step S162) the process extracts the authentication key, which has been assigned to the user, from the database 166 and transmits it to the ASP 500 of the LSM 230 (step S165). Thereafter, the process of the present invention proceeds to step S180 in Fig. 3.

Fig. 5 is a flowchart illustrating the banner transmission process shown in Fig. 3.

If the user is determined as a non-paying one (step S150), the process searches the non-paying user database 176(step S171) to determine whether the user is a new one (step S172). If so, the process transmits basic banner information to the ASP 500 of the LSM 230 (step S173). In a subsequent step S174, the process registers information of the LSM 230 including a host name and IP address in the database 176 and proceeds to step S180 in Fig. 3. If the user was determined as a previously registered one (step S172), the process provides banner information assigned to the user or that to be changed to the ASP 500 (step S175) and proceeds step S180 in Fig. 3.

Fig. 6 is a flowchart which will be used to describe the operation of the ASP 500 shown in Fig. 2.

Upon the reception of a stand-by signal from the remote controller 160 (step S200), the ASP 500 performs a preparatory task for execution of application services such as a TCP/IP protocol implementation and daemon execution (step S210). Subsequently, it receives data that was previously set according to a user type from the remote controller 160. Specifically, the process downloads banner information for a non-paying user (step S220) and receives the authentication key for a paying user (step S230). Thereafter, the process transmits data

obtained at steps S220 and S230 to the remote controller 160, wherein an accuracy of the data is checked (step S240). Next, upon the reception of the execution permission signal from the remote controller 160, the process executes the application program 510 (step S260) and is terminated. In this case, if the user is non-paying one, the process transmits the banner advertisement (step S270) based on the banner information downloaded at step S220. If none of the execution permission signal is received, the process is terminated.

If the application program 510 is launched in the LSM 230 of the user module 200 through the above steps shown in Figs. 3 to 6, the subsequent control of the application program 510 is performed by the LSM 230. Specifically, the ASP data center 100 has nothing to do with the use of the application program 510 until a certain event occurs. The "certain event" signifies that the user breaks the contract with the ASP data center 100 or the contract expires. Upon an occurrence of such event, the ASP data center 100 may connect to the application control module 520 of the LSM 230 to change or delete the application program 510. In addition, application programs, which are being launched in the LSM 230 of the user module 200, may be operated without being controlled by the ASP data center 100 unless an aforementioned certain event occurs. In this case, even if communications between the user module 200 and the ASP data center 100 are disconnected, the application programs in the user module 200 are uninterruptedly operated, thereby allowing a stable application service.

On the other hand, the ASP data center 100 can monitor the status of the ASP 500, if desired. For example, the monitoring includes a zero defect inspection and change of the banner provided to the non-paying user, or a verification of the authentication key provided to the paying user. The monitoring may be applied to a

certain application downloaded from the ASP data center 100.

Fig. 7 is a flowchart which will be used to describe the monitoring procedure between the ASP data center 100 and the ASPs 500 and 501.

The ASP data center 100 transmits a monitoring start signal to the ASPs 500 and 501 to monitor a status of them (step S700). Each of the ASPs 500 and 501, responsive to the monitoring start signal, transmits an authentication key and a banner advertisement assigned to each and attributes information for the downloaded file to the ASP data center 100 (step S710). The ASP data center 100 compares first information provided when each of the ASPs 500 and 501 is installed in the LSMs 230 and 240 with second information transmitted from the above step S710 (step S720). An authorized or unauthorized use is determined according to the comparison result (step S720). Specifically, if the result founds an unauthorized use, the ASP data center 100 collects a list of the LSMs (step S730), and changes, controls or stops execution of application programs installed in the LSMs with the unauthorized use (step S740).

With the above-described configuration and referring to Fig. 2, the end users 201-204, which are connected to the user module 200 as a member via a local network 235 such as LAN and Ethernet, connect to the LSM 230 in order to enjoy a desired ASP service. In other words, as various ASP programs are installed in the LSM 230, the end users 201 to 204 only need to connect to the LSM 230 assigned to them in order to use the ASP service. There is no need to directly connect to the ASP data center 100. Similarly, the end users 211-214 connect to their assigned ASP 501 of the LSM 240 via the local network 245 in order to select a desired application service. Meanwhile, a remotely-located user 600 who is not connected with the LSMs 230 and 240 can connect to

any one of the LSMs 230 and 240 via a communication network such as the Internet in order to use the application service.

As mentioned above, in accordance with the present invention, the transfer of data generated from each of the user modules 200 and 210 is processed at the LSMs 230 and 240, thereby distributing a significant amount of traffic that was conventionally concentrated at a centralized area.

Furthermore, the present invention allows ASP providers to recycle the local storage medium of the user modules, the local network equipments, maintenance manpower, communication channels, thereby removing requirements of equipments such as customer servers, application servers, workstations, LANs, security and backup facilities, which, in turn, saves a significant amount of prior investment cost for the ASP business. In addition, the present invention allows banner advertisements to be provided to the user to be changed in a real time at an ASP data center, thereby maximizing efficiency of the banner advertisements.

Moreover, the present invention allows a user to utilize its own local storage media without purchasing or renting a separate local storage media, thereby saving purchase and rental costs, and allows queries generated at a local to be processed thereat, thereby improving a service processing speed, which is turn, provides a stable application service. Furthermore, the present invention allows management of end user accounts to be performed at the local storage media, thereby having none of the requirement of the provision of the user account information to an ASP provider, or a contract management for an information storage media, which, in turn, prevents user information from being drained externally.

While the invention has been described with reference to its preferred embodiments, it will be

apparent to those skilled in the art that variations and modifications are possible without deviating from the broad principles and teachings of the present invention which should be limited solely by the scope of the claims appended hereto.

CLAIMS

1. A system for providing at least one of application services to a user, comprising:

means, disposed in a user module, for providing at least one of application services to the user; and

means, remotely located to the user module, for controlling the application services, and

wherein application service data associated with the application services is stored in the providing means, and

wherein the providing means is initially operated under the control of the controlling means, and is operated independent of the controlling means after the initial operation.

2. The system of claim 1, wherein the providing means, after the initial operation, is in operation independent of the controlling means until it receives an execution prohibition signal from the controlling means.

3. The system of claim 1, wherein the controlling means includes:

means for storing information on a local storage media (LSM) of the user module; and

means for transmitting a predetermined control signal to the providing means based on the LSM information, when it receives a signal requesting the execution of the providing means from the user.

4. The system of claim 3, wherein the controlling means further includes means for changing and deleting the application service data stored in the providing means, if desired.

5. The system of claim 3, wherein the predetermined

control signal includes at least one of a signal representing whether the execution of the application services is permitted, a predetermined authentication key signal assigned to the user, and a preset advertisement signal, wherein the authentication key is stored in the storing means.

6. The system of claim 3, wherein the controlling means further includes means for comparing the predetermined control signal transmitted thereto from the providing means with a previous control signal, thereby determining whether or not the control signals are equal with one another.

7. The system of claim 3, wherein the controlling means further includes means for classifying the users into a predefined type to selectively provide the predetermined control signal based on the predefined type.

8. The system of claim 7, wherein the predefined type is sorted according to whether the user pays a rental fee for the application service provided from the providing means.

9. The system of claim 8, wherein the application service data includes at least one of a software-based application program and solution.

10. A method, in an application service system including a controller with a user database of storing information on a plurality of users therein and a user module having at least one of application service data, for remotely controlling the execution of the application service data using a communication network, comprising the steps of:

(a) receiving a service request of the application

service data from a user via the network;

(b) determining whether the user's information contained in the service request is valid based on the user information stored in the user database;

(c) transmitting a control signal containing a service permission or prohibition signal for the application service data to the user module, according to the determined result at the above step (b); and

(d) allowing, the user module, responsive to the control signal, to control the access of the user to the application service data.

11. The method of claim 10, wherein the control signal includes at least one of a signal for permitting the access of the user to the application service data, a signal for prohibiting the access of the user to the application service data, an authentication key signal assigned to the user, and a preset advertisement signal previously registered in the system.

12. The method of claim 11, wherein the user module, after the application service data is launched based on the access permission signal, maintains the execution state until it receives the execution prohibition signal from the controller.

13. The method of claim 12, wherein the application service data includes at least one of a software-based application program and solution.

14. The method of claim 10, wherein the step (b) further includes the step of classifying the user into a predefined type to selectively provide the control signal based on the predefined type.

15. The method of claim 14, wherein the predefined type

is sorted according to whether the user pays a rental fee for the application service provided from the providing means.

16. The method of claim 14, wherein the authentication key is transmitted to the user module when the user is a paid one; and the advertisement signal is transmitted to the user module when the user is a free one.

17. The method of claim 10, wherein the controller changes or deletes the application service data based on the determined result, if desired.

18. The method of claim 14, wherein when the user is the paid one, the step (b) further includes:

(b1) storing information on the paid user in the user database;

(b2) checking whether or not the user is a new one based on the paid user's information stored in the user database;

(b3) creating, when the user is a new one, a new authentication key using the user's information, transmitting it to the user module, and storing the transmitted authentication key data in the user database; and

(b4) extracting, when the user is a pre-registered one, an authentication key previously assigned to the user from the user database and transmitting it to the user module.

19. The method of claim 14, wherein when the user is the free one, the step (b) further includes:

(b11) storing information on the free user in the user database;

(b21) checking whether or not the user is a new one based on the free user's information stored in the user

database;

(b31) transmitting, when the user is a new one, the advertisement signal to the user module; and

(b41) transmitting, when the user is a pre-registered one, advertisements previously assigned to the user or a new advertisement to be replaced to the user module.

FIG. 1

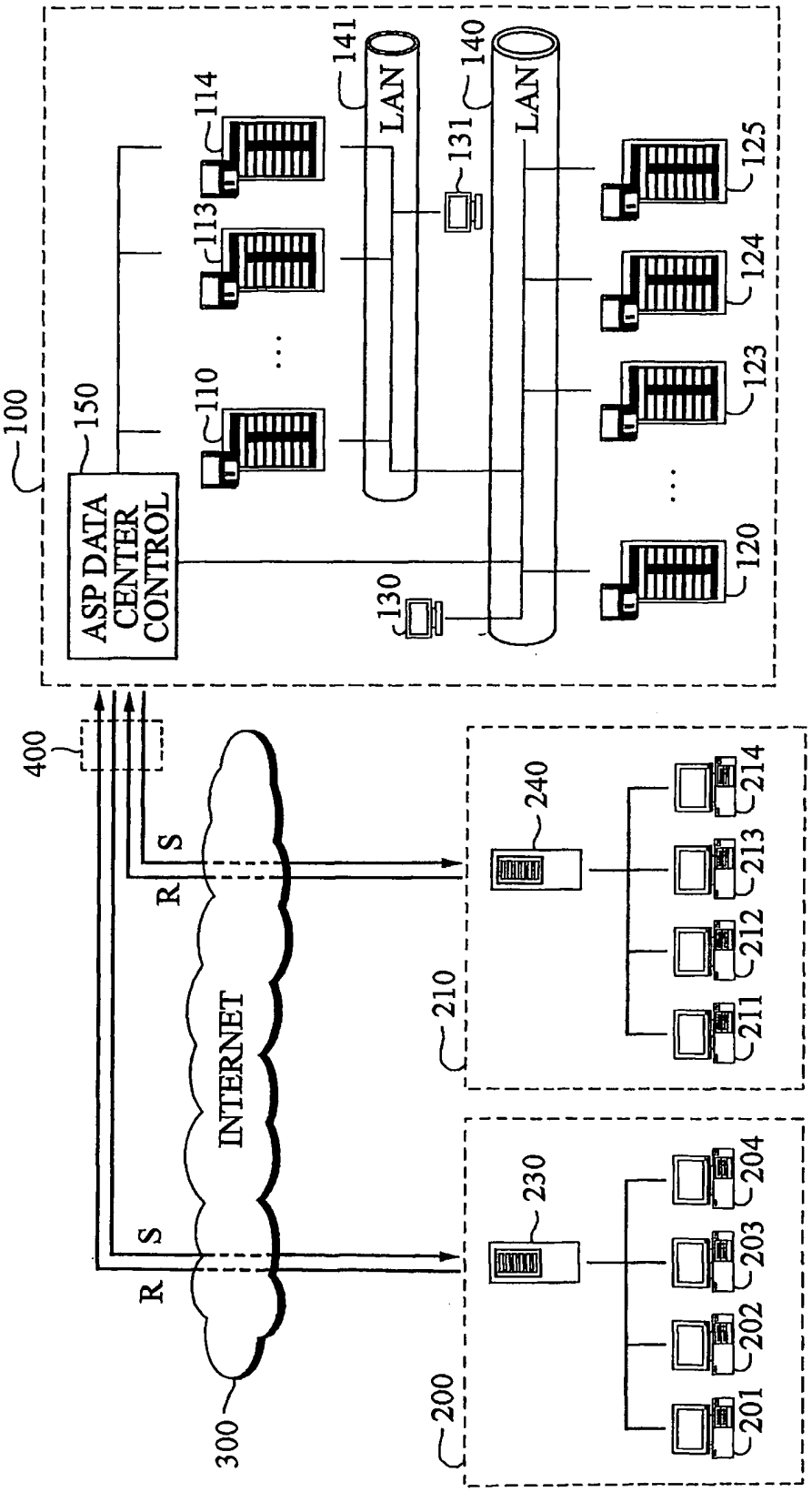

100
150
ASP DATA CENTER CONTROL
110
113
114
141
LAN
131
140
LAN
120
123
124
125
130
400
S
R
S
R
INTERNET
300
200
201
202
203
204
230
210
211
212
213
214
240

FIG. 2

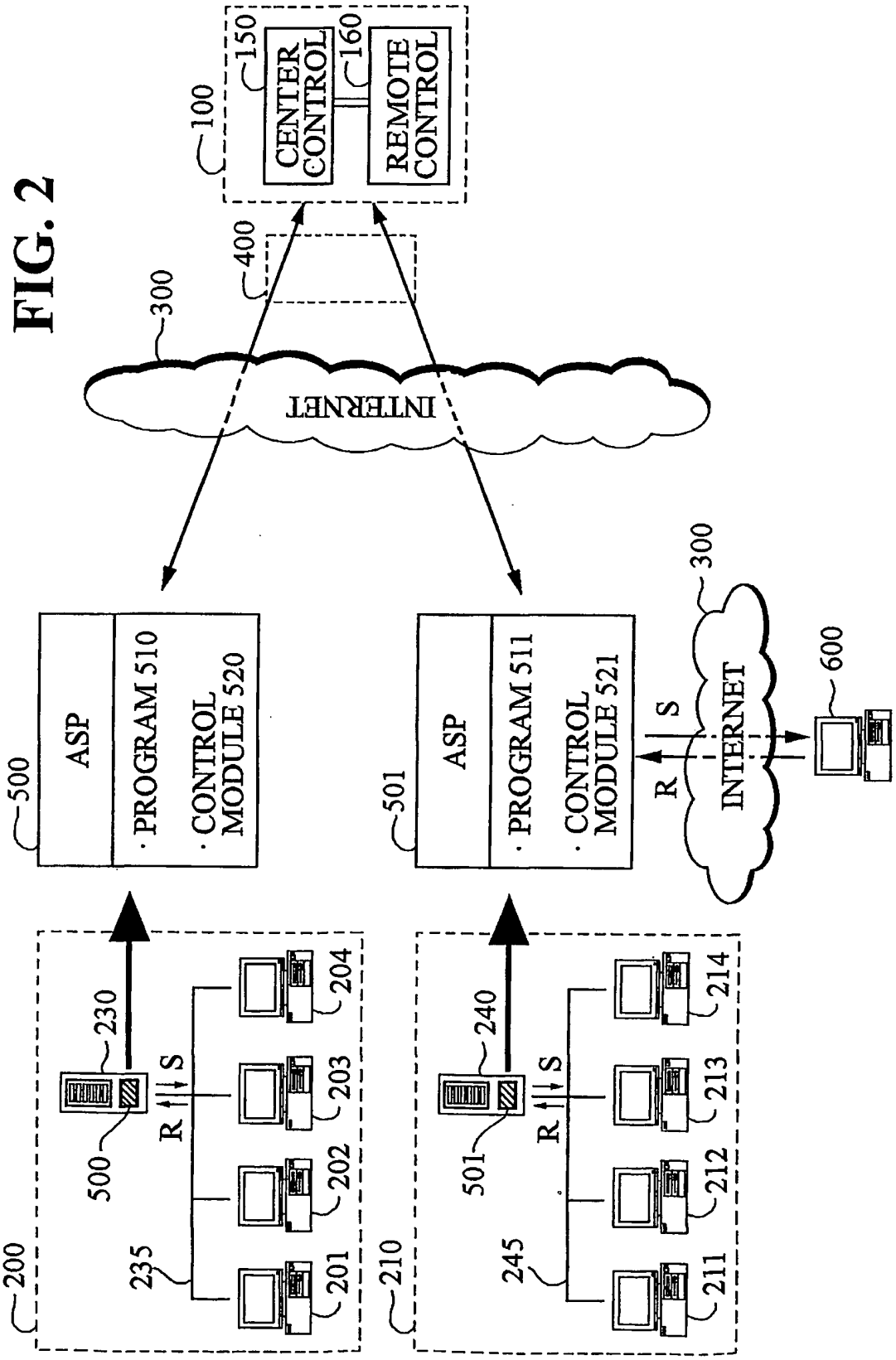

100
150
CENTER CONTROL
160
REMOTE CONTROL
400
300
INTERNET
500
ASP
· PROGRAM 510
· CONTROL MODULE 520
501
ASP
· PROGRAM 511
· CONTROL MODULE 521
300
INTERNET
600
R
S
200
230
500
R
S
235
201
202
203
204
210
240
501
R
S
245
211
212
213
214

FIG. 3

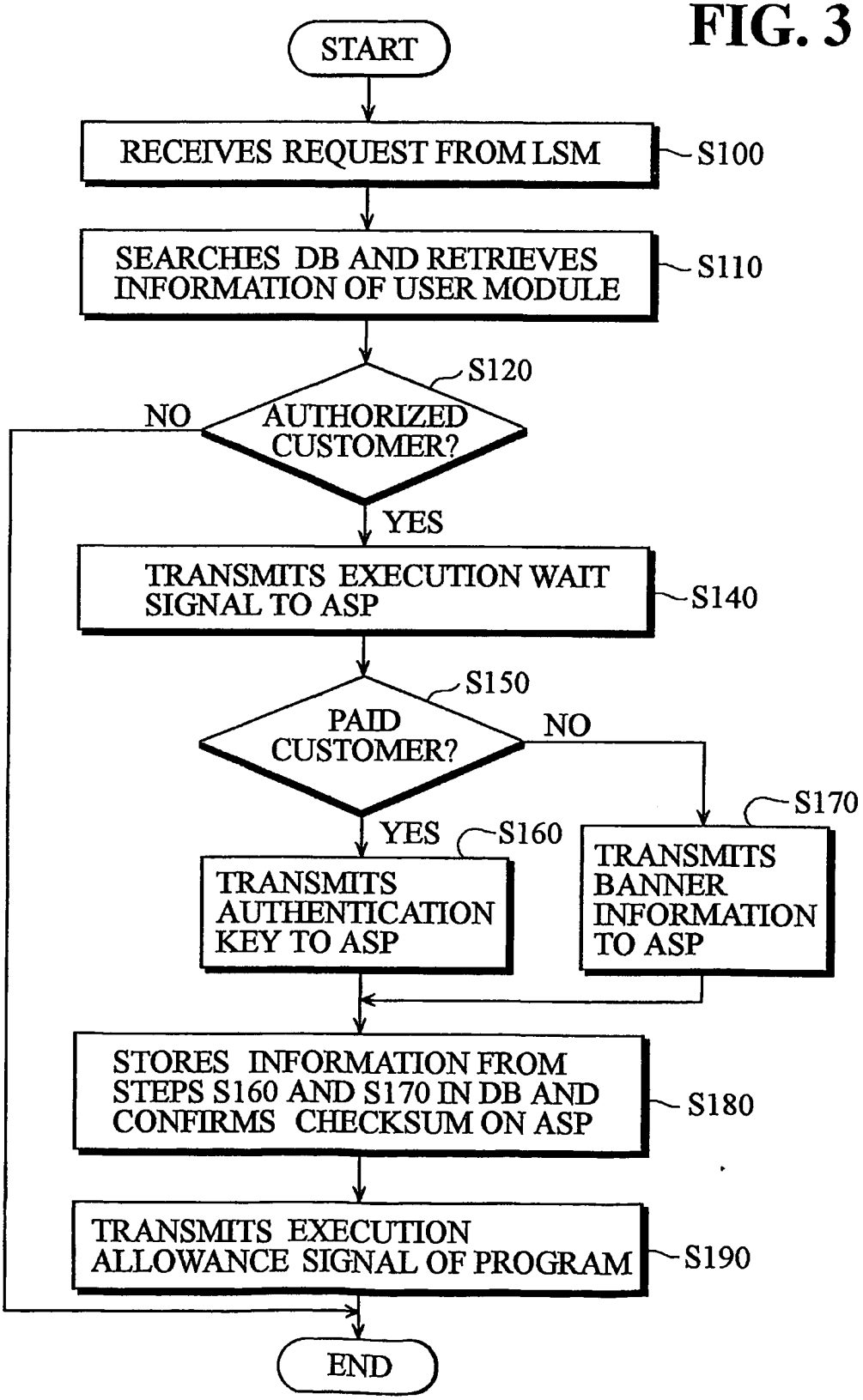

START
RECEIVES REQUEST FROM LSM
S100
SEARCHES DB AND RETRIEVES INFORMATION OF USER MODULE
S110
S120
AUTHORIZED CUSTOMER?
NO
YES
TRANSMITS EXECUTION WAIT SIGNAL TO ASP
S140
S150
PAID CUSTOMER?
NO
YES
S160
TRANSMITS AUTHENTICATION KEY TO ASP
S170
TRANSMITS BANNER INFORMATION TO ASP
STORES INFORMATION FROM STEPS S160 AND S170 IN DB AND CONFIRMS CHECKSUM ON ASP
S180
TRANSMITS EXECUTION ALLOWANCE SIGNAL OF PROGRAM
S190
END

FIG. 4

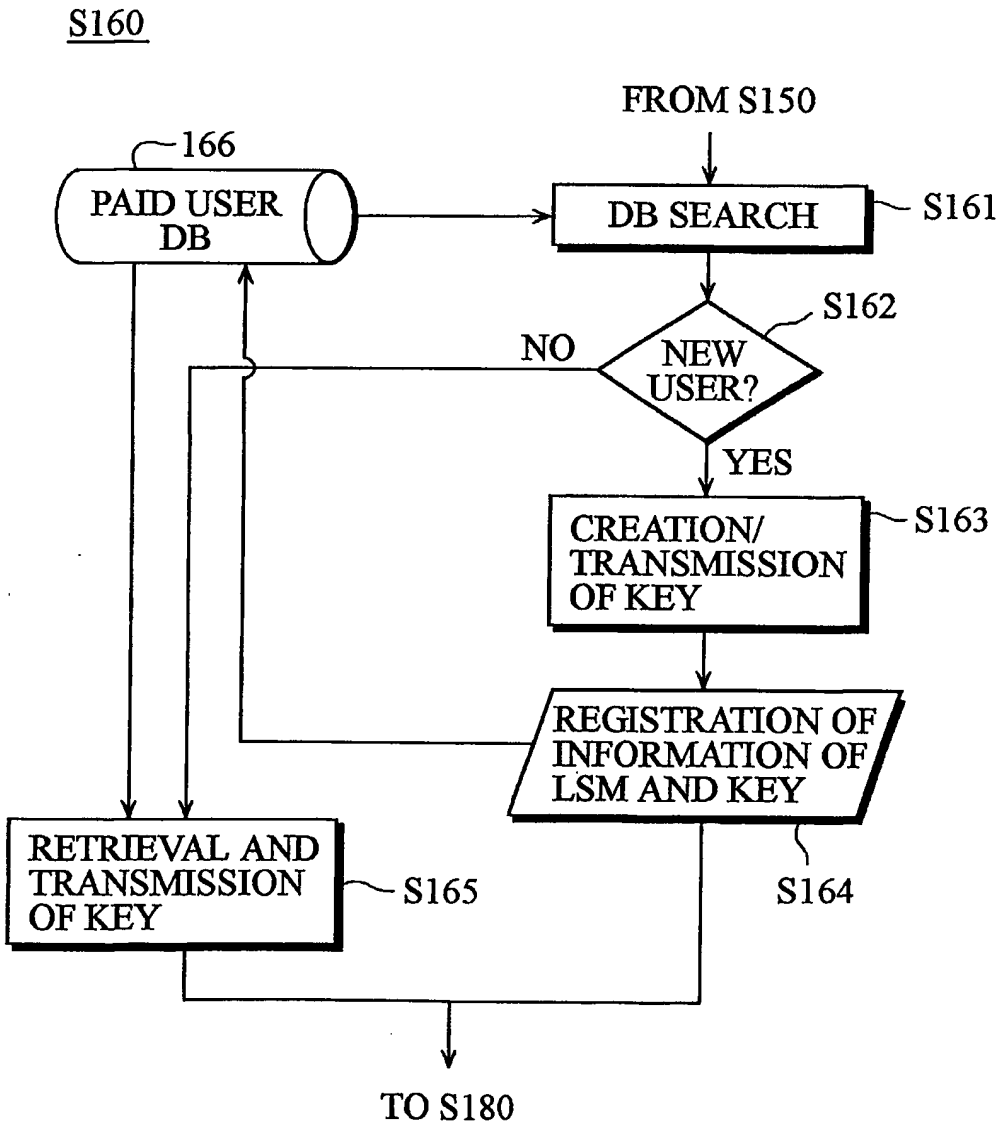

S160
FROM S150
166
PAID USER DB
DB SEARCH
S161
S162
NEW USER?
NO
YES
CREATION/ TRANSMISSION OF KEY
S163
REGISTRATION OF INFORMATION OF LSM AND KEY
S164
RETRIEVAL AND TRANSMISSION OF KEY
S165
TO S180

FIG. 5

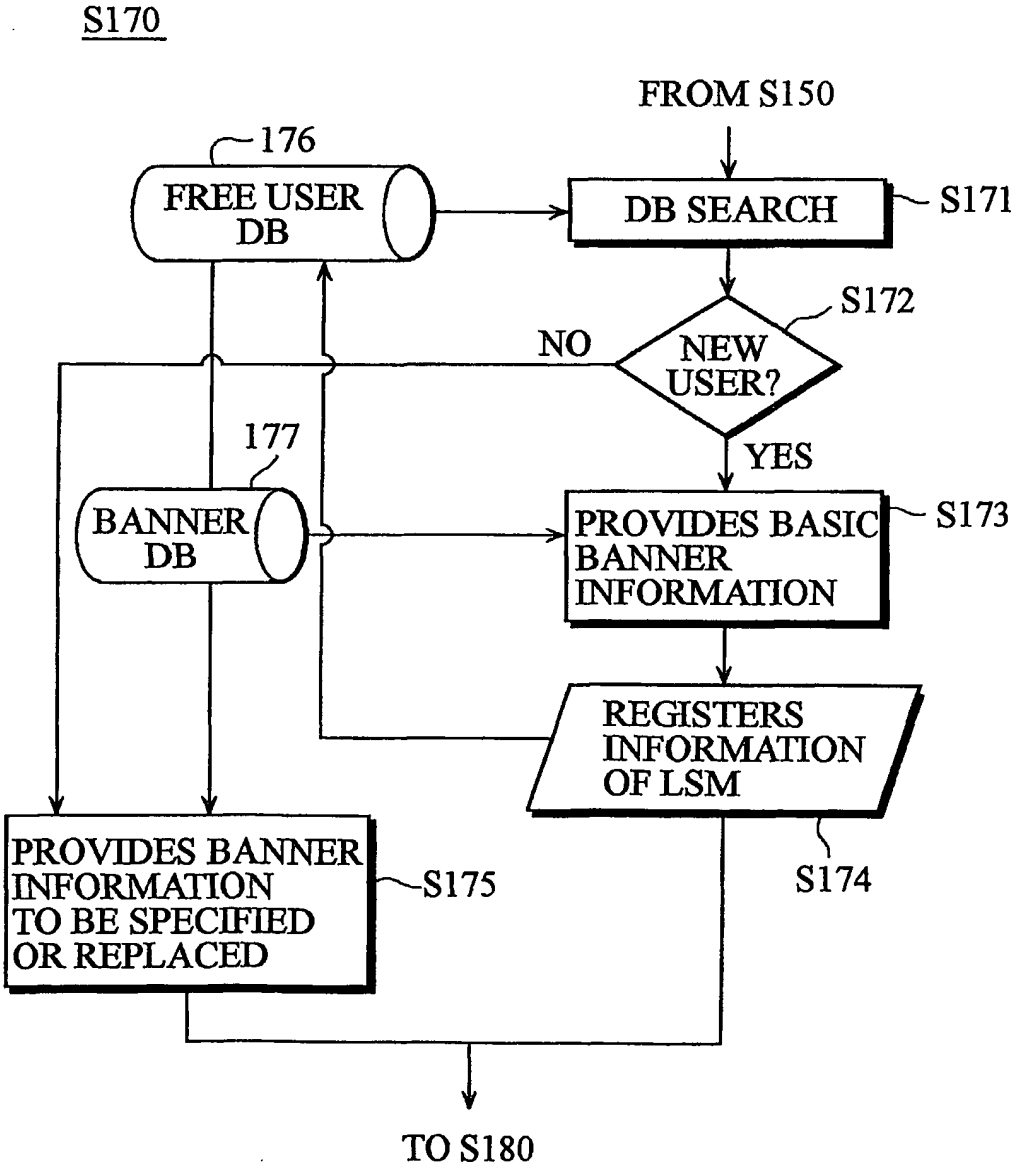

S170
FROM S150
176
FREE USER DB
DB SEARCH
S171
S172
NO
NEW USER?
YES
177
BANNER DB
PROVIDES BASIC BANNER INFORMATION
S173
REGISTERS INFORMATION OF LSM
S174
PROVIDES BANNER INFORMATION TO BE SPECIFIED OR REPLACED
S175
TO S180

FIG. 6

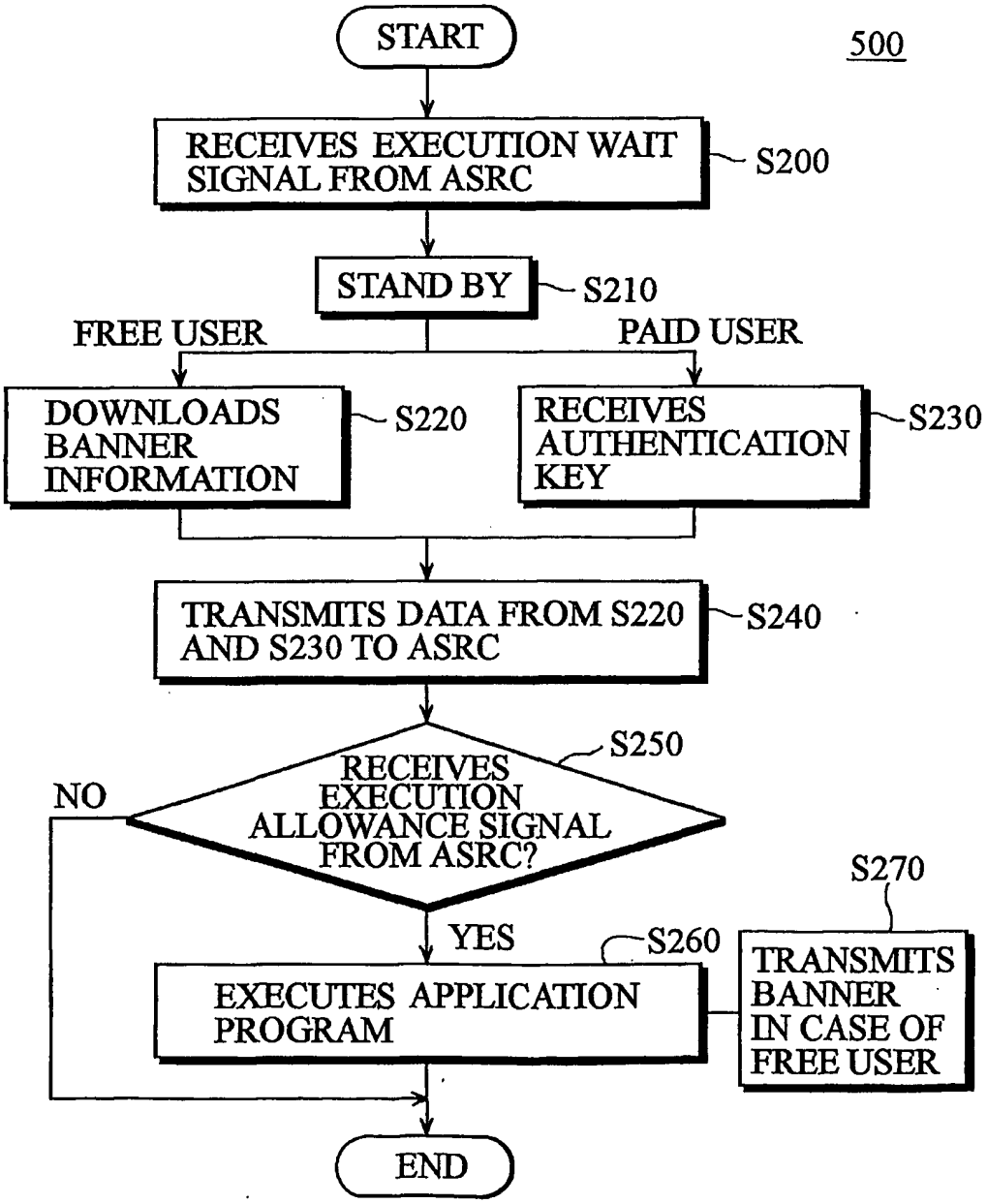
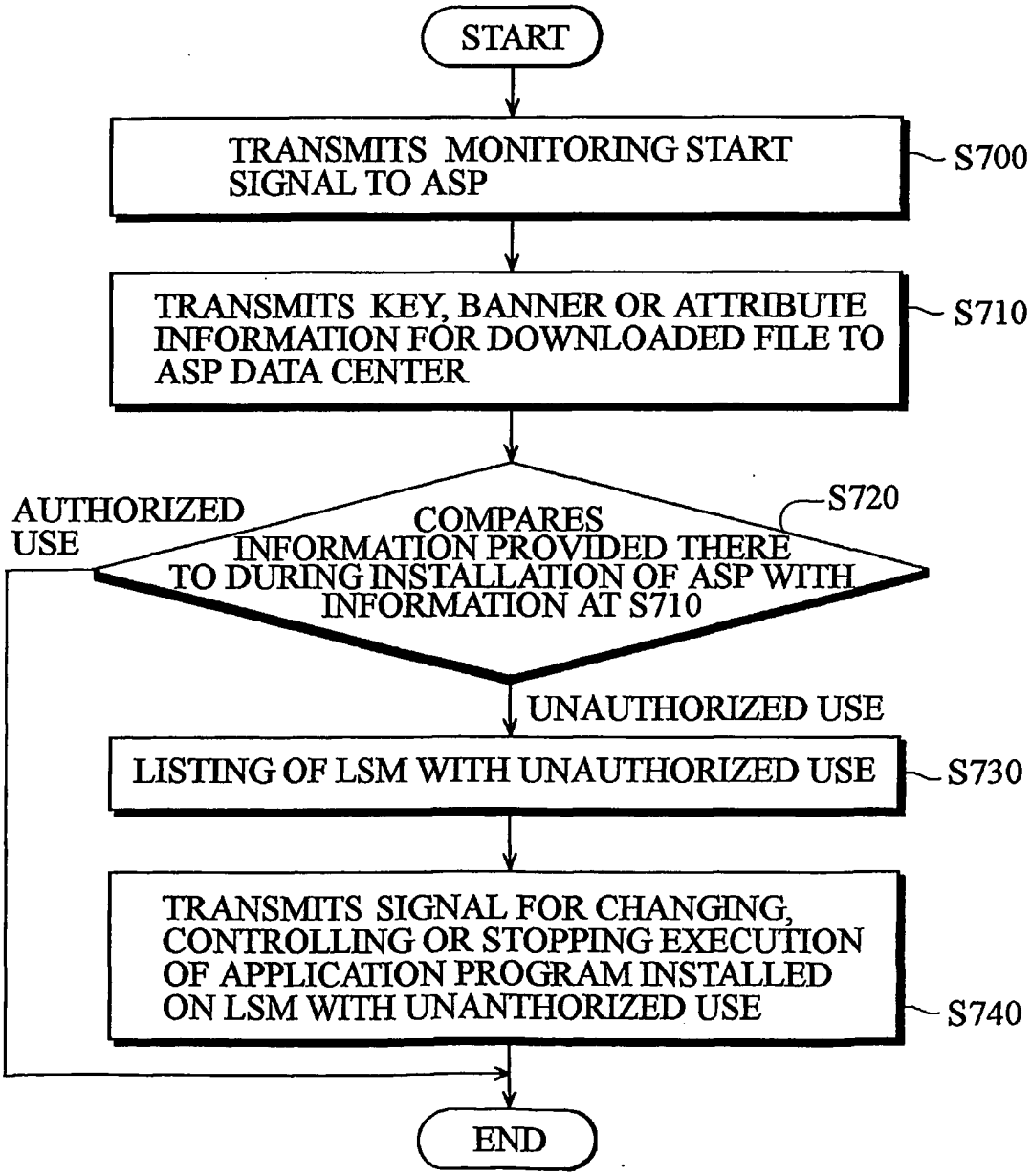

START
500
RECEIVES EXECUTION WAIT SIGNAL FROM ASRC
S200
STAND BY
S210
FREE USER
PAID USER
DOWNLOADS BANNER INFORMATION
S220
RECEIVES AUTHENTICATION KEY
S230
TRANSMITS DATA FROM S220 AND S230 TO ASRC
S240
RECEIVES EXECUTION ALLOWANCE SIGNAL FROM ASRC?
S250
NO
YES
EXECUTES APPLICATION PROGRAM
S260
TRANSMITS BANNER IN CASE OF FREE USER
S270
END

FIG. 7


START
TRANSMITS MONITORING START SIGNAL TO ASP
S700
TRANSMITS KEY, BANNER OR ATTRIBUTE INFORMATION FOR DOWNLOADED FILE TO ASP DATA CENTER
S710
COMPARES INFORMATION PROVIDED THERE TO DURING INSTALLATION OF ASP WITH INFORMATION AT S710
S720
AUTHORIZED USE
UNAUTHORIZED USE
LISTING OF LSM WITH UNAUTHORIZED USE
S730
TRANSMITS SIGNAL FOR CHANGING, CONTROLLING OR STOPPING EXECUTION OF APPLICATION PROGRAM INSTALLED ON LSM WITH UNANTHORIZED USE
S740
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR01/01293

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 G06F 17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimun documentation searched (classification system followed by classification symbols)

G06F 15/00, 17/60

Documentation searched other than minimun documentation to the extent that such documents are included in the fileds searched

KOREAN PATENTS AND APPLICATIONS FOR INVENTIONS SINCE 1975
KOREAN UTILITY MODELS AND APPLICATIONS FOR UTILITY MODELS SINCE 1975

Electronic data base consulted during the intertnational search (name of data base and, where practicable, search trerms used)

HTTP://WWW.USPTO.GOV/
WPI, PAJ, IEEE/IEE ELECTRONIC LIBRARY(1998) 'APPLICATION AND SERVICE AND PROVIDER'

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US-6061516 (Hitachi, Ltd.) May. 9, 2000 * Whole Document *	1
A	US-5734828 (Intel Corporation) March. 31, 1998 * Whole Document *	1
A	US-6047273 (Vaghi Family Intellectual Property) April. 4, 2000 * Whole Document *	1
A	US-6018570 (Nynex Science and Technology Inc.) Jan. 25, 2000 * Whole Document *	1
A	US-6041346 (Ateon Networks, Inc.) * Whole Document *	1

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevence
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevence; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevence; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 NOVEMBER 2001 (12.11.2001)	14 NOVEMBER 2001 (14.11.2001)

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office Government Complex-Daejeon, Dunsan-dong, Seo-gu, Daejeon Metropolitan City 302-701, Republic of Korea	YANG, In Soo
Facsimile No. 82-42-472-7140	Telephone No. 82-42-481-5782